



1 Mona Amini, Esq.  
Nevada Bar No. 15381  
2 Gustavo Ponce, Esq.  
Nevada Bar No. 15084  
3 **KAZEROUNI LAW GROUP, APC**  
6940 S. Cimarron Road, Suite 210  
4 Las Vegas, Nevada 89113  
Telephone: (800) 400-6808  
5 Facsimile: (800) 520-5523  
E-mail: mona@kazlg.com  
6 E-mail: gustavo@kazlg.com

7 Mason A. Barney, Esq. *\*pro hac vice forthcoming*  
Tyler J. Bean, Esq. *\*pro hac vice forthcoming*  
8 **SIRI & GLIMSTAD LLP**  
745 Fifth Avenue, Suite 500  
9 New York, New York 10151  
Telephone: (212) 532-1091  
10 E-mail: mbarney@sirillp.com  
E-mail: tbean@sirillp.com

11 *Attorneys for Plaintiff,*  
12 Tracy Cowherd

13 **UNITED STATES DISTRICT COURT**  
14 **FOR THE DISTRICT OF NEVADA**

15 TRACY COWHERD, individually and on  
behalf of all similarly situated persons,

16 Plaintiff,

17 vs.  
18

19 MY DAILY CHOICE, INC.,

20 Defendant.  
21  
22  
23  
24

Case No.:

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

25 //

26 //

27 //

28 //

1 Plaintiff Tracy Cowherd (“Plaintiff”), individually and on behalf of all  
2 similarly situated persons, alleges the following against My Daily Choice Inc.,  
3 (“MDC” or “Defendant”) based upon personal knowledge with respect to herself and  
4 on information and belief derived from, among other things, investigation by her  
5 counsel and review of public documents as to all other matters:

### 6 **INTRODUCTION**

7 1. Plaintiff brings this class action against MDC for its failure to properly  
8 secure and safeguard Plaintiff’s and other similarly situated MDC customers’  
9 payment card information (the “Private Information”) from hackers.

10 2. MDC, based in Las Vegas, markets and sells various consumer products  
11 and services through its website and affiliates that serve thousands of customers  
12 nationwide.

13 3. On or about June 17, 2024, MDC filed official notice of a hacking  
14 incident with the Office of the Maine Attorney General.

15 4. On or about June 5, 2024, MDC also sent out data breach letters to  
16 individuals whose information was compromised as a result of the hacking incident.

17 5. Based on the Notice filed by the company, on February 15, 2024, MDC  
18 detected unusual activity on its third-party vendor’s computer systems. In response,  
19 the company launched an investigation. The MDC investigation revealed that an  
20 unauthorized party had access to certain company files on February 15, 2024 (the  
21 “Data Breach”). Yet, MDC waited more than three months to notify the public that  
22 they were at risk.

23 6. As a result of this delayed response, Plaintiff and “Class Members”  
24 (defined below) had no idea for more than three months that their Private Information  
25 had been compromised, and that they were, and continue to be, at significant risk of  
26 identity theft and various other forms of personal, social, and financial harm. The risk  
27 will remain for their respective lifetimes.

1           7.     The Private Information compromised in the Data Breach included  
2 highly sensitive data that represents a gold mine for data thieves, including but not  
3 limited to, names, dates of birth, Social Security numbers, driver's license numbers,  
4 state identification numbers, passport numbers, financial account information, digital  
5 signatures, medical information, health insurance information, biometric information,  
6 and mother's maiden names that MDC collected and maintained.

7           8.     Armed with the Private Information accessed in the Data Breach, data  
8 thieves can commit a variety of crimes including, *e.g.*, identity theft and financial  
9 fraud.

10          9.     There has been no assurance offered by MDC that all personal data or  
11 copies of data have been recovered or destroyed, or that Defendant has adequately  
12 enhanced its data security practices sufficient to avoid a similar breach in the future.

13          10.    Therefore, Plaintiff and Class Members have suffered and are at an  
14 imminent, immediate, and continuing increased risk of suffering ascertainable losses  
15 in the form of harm from identity theft and other fraudulent misuse of their Private  
16 Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred  
17 to remedy or mitigate the effects of the Data Breach, and the value of their time  
18 reasonably incurred to remedy or mitigate the effects of the Data Breach.

19          11.    Plaintiff brings this class action lawsuit to address MDC's inadequate  
20 safeguarding of Class Members' Private Information that it collected and maintained,  
21 and its failure to provide timely and adequate notice to Plaintiff and Class Members  
22 of the types of information that were accessed, and that such information was subject  
23 to unauthorized access by cybercriminals.

24          12.    The potential for improper disclosure and theft of Plaintiff's and Class  
25 Members' Private Information was a known risk to MDC, and thus MDC was on  
26 notice that failing to take necessary steps to secure the Private Information left it  
27 vulnerable to an attack.

28

16. Accordingly, Plaintiff, on behalf of herself and the Class, asserts claims for negligence, negligence per se, breach of contract, breach of implied contract, invasion of privacy, unjust enrichment, and declaratory judgment.

18. Defendant MDC is an online retailer that markets and sells various consumer products and services through its website with its principal place of business at 6713 South Eastern Ave, Las Vegas, Nevada, 89119.

20. This Court has jurisdiction over MDC because MDC operates in and/or is incorporated in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and MDC has harmed Class Members residing in this District.

### **FACTUAL ALLEGATIONS**

#### ***MDC's Business and Collection of Plaintiff's and Class Members' Private Information***

22. MDC is an online retailer that markets and sells various consumer products and services through its website. Founded in 2014, MDC provides consumer goods and services in health and wellness, apparel, cosmetics, and financial management throughout the United States, serving more than 89,000 customers. MDC employs more than 92 people and generates hundreds of millions in annual revenue.

23. As a condition of receiving consumer goods and services, MDC requires that its customers entrust it with highly sensitive personal information. In the ordinary course of receiving service from MDC, Plaintiff and Class Members were required to provide their Private Information to Defendant.

24. MDC uses this information, *inter alia*, for marketing, shipping, and processing purposes.

25. In its privacy statement, MDC promises its customers that it will “take appropriate security measures to protect your personal data and we demand the same from parties who process personal data on our behalf.”<sup>1</sup>

We take security measures to reduce misuse of and unauthorized access to personal data. We take the following measures in particular:

- Access to personal data requires the use of a username and password.
- Access to personal data requires the use of a username and login token.
- After receipt, the data will be stored in our proprietary database servers.

<sup>1</sup> See <https://mydailychoice.com/privacy-policy> (last visited June 17, 2024).

- We take physical measures to protect access to the systems in which the personal data is stored.
- We make use of secure connections (Secure Sockets Layer of SSL) to encrypt all information between you and our website when entering your personal data.
- We keep logs of all requests for personal data.<sup>2</sup>

26. Because of the highly sensitive and personal nature of the information MDC acquires and stores with respect to its customers, MDC, upon information and belief, promises to, among other things: keep customers' Private Information private; comply with industry standards related to data security and the maintenance of its customers' Private Information; inform its customers of its legal duties relating to data security and comply with all federal and state laws protecting customers' Private Information; only use and release customers' Private Information for reasons that relate to the services it provides; and provide adequate notice to customers if their Private Information is disclosed without authorization.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, MDC assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

28. Plaintiff and Class Members relied on MDC to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

***The Data Breach and MDC's Inadequate Notice to Plaintiff and Class Members***

29. According to Defendant's Notice, it learned of unauthorized access to its vendor's computer systems on February 15, 2024, with such unauthorized access having taken place on February 15, 2024.

---

<sup>2</sup> *Id.*

1        30. Through the Data Breach, the unauthorized cybercriminal(s) accessed a  
2 cache of highly sensitive Private Information, including names, dates of birth, Social  
3 Security numbers, driver's license numbers, state identification numbers, passport  
4 numbers, financial account information, digital signatures, medical information,  
5 health insurance information, biometric information, and mother's maiden names.

6        31. On or about June 5, 2024, roughly three months after MDC learned that  
7 the Class's Private Information was first accessed by cybercriminals, MDC finally  
8 began to notify customers that its investigation determined that their Private  
9 Information was impacted.

10        32. MDC delivered Data Breach Notification Letters to Plaintiff and Class  
11 Members, alerting them that their highly sensitive Private Information had been  
12 exposed in an "incident."

13        33. The notice letter then attached some pages entitled "Steps You Can Take  
14 To Protect Personal Information," which listed generic steps that victims of data  
15 security incidents can take, such as getting a copy of a credit report or notifying law  
16 enforcement about suspicious financial account activity. Other than providing  
17 instructions to obtain a credit report and a call center number that victims could  
18 contact "with any questions," MDC offered no other substantive steps to help victims  
19 like Plaintiff and Class Members to protect themselves. On information and belief,  
20 MDC sent a similar generic letter to all individuals affected by the Data Breach.

21        34. MDC had obligations created by contract, industry standards, common  
22 law, and representations made to Plaintiff and Class Members to keep Plaintiff's and  
23 Class Members' Private Information confidential and to protect it from unauthorized  
24 access and disclosure.

25        35. Plaintiff and Class Members provided their Private Information to MDC  
26 with the reasonable expectation and mutual understanding that MDC would comply  
27 with its obligations to keep such information confidential and secure from  
28 unauthorized access and to provide timely notice of any security breaches.



1        36. MDC’s data security obligations were particularly important given the  
2 substantial increase in cyberattacks in recent years.

3        37. MDC knew or should have known that its electronic records would be  
4 targeted by cybercriminals.

5 ***MDC Failed to Comply with FTC Guidelines***

6        38. The Federal Trade Commission (“FTC”) has promulgated numerous  
7 guides for businesses which highlight the importance of implementing reasonable  
8 data security practices. According to the FTC, the need for data security should be  
9 factored into all business decision making. Indeed, the FTC has concluded that a  
10 company’s failure to maintain reasonable and appropriate data security for  
11 consumers’ sensitive personal information is an “unfair practice” in violation of  
12 Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. *See, e.g.,*  
13 *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

14        39. In October 2016, the FTC updated its publication, *Protecting Personal*  
15 *Information: A Guide for Business*, which established cybersecurity guidelines for  
16 businesses. The guidelines note that businesses should protect the personal customer  
17 information that they keep, properly dispose of personal information that is no longer  
18 needed, encrypt information stored on computer networks, understand their network’s  
19 vulnerabilities, and implement policies to correct any security problems. The  
20 guidelines also recommend that businesses use an intrusion detection system to  
21 expose a breach as soon as it occurs, monitor all incoming traffic for activity  
22 indicating someone is attempting to hack into the system, watch for large amounts of  
23 data being transmitted from the system, and have a response plan ready in the event  
24 of a breach.

25        40. The FTC further recommends that companies not maintain personally  
26 identifiable information (“PII”) longer than is needed for authorization of a  
27 transaction, limit access to sensitive data, require complex passwords to be used on  
28 networks, use industry-tested methods for security, monitor the network for



1 suspicious activity, and verify that third-party service providers have implemented  
2 reasonable security measures.

3 41. The FTC has brought enforcement actions against businesses for failing  
4 to adequately and reasonably protect customer data by treating the failure to employ  
5 reasonable and appropriate measures to protect against unauthorized access to  
6 confidential consumer data as an unfair act or practice prohibited by the FTCA.  
7 Orders resulting from these actions further clarify the measures businesses must take  
8 to meet their data security obligations.

9 42. As evidenced by the Data Breach, MDC failed to properly implement  
10 basic data security practices. MDC's failure to employ reasonable and appropriate  
11 measures to protect against unauthorized access to Plaintiff's and Class Members'  
12 Private Information constitutes an unfair act or practice prohibited by Section 5 of the  
13 FTCA.

14 43. MDC was at all times fully aware of its obligation to protect the Private  
15 Information of its customers yet failed to comply with such obligations. Defendant  
16 was also aware of the significant repercussions that would result from its failure to do  
17 so.

18 ***MDC Failed to Comply with Industry Standards***

19 44. As noted above, experts studying cybersecurity routinely identify  
20 businesses as being particularly vulnerable to cyberattacks because of the value of the  
21 Private Information which they collect and maintain.

22 45. Some industry best practices that should be implemented by businesses  
23 like MDC include but are not limited to educating all employees, strong password  
24 requirements, multilayer security including firewalls, anti-virus and anti-malware  
25 software, encryption, multi-factor authentication, backing up data, and limiting which  
26 employees can access sensitive data. As evidenced by the Data Breach, Defendant  
27 failed to follow some or all of these industry best practices.

28

1        46. Other best cybersecurity practices that are standard in the industry  
2 include: installing appropriate malware detection software; monitoring and limiting  
3 network ports; protecting web browsers and email management systems; setting up  
4 network systems such as firewalls, switches, and routers; monitoring and protecting  
5 physical security systems; and training staff regarding these points. As evidenced by  
6 the Data Breach, Defendant failed to follow these cybersecurity best practices.

7        47. Defendant failed to meet the minimum standards of any of the following  
8 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without  
9 limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1,  
10 PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8,  
11 and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS  
12 CSC), which are all established standards in reasonable cybersecurity readiness.

13        48. Defendant failed to comply with these accepted standards, thereby  
14 permitting the Data Breach to occur.

15 ***MDC Breached its Duty to Safeguard Plaintiff's and Class Members' Private***  
16 ***Information***

17        49. In addition to its obligations under federal and state laws, MDC owed a  
18 duty to Plaintiff and Class Members to exercise reasonable care in obtaining,  
19 retaining, securing, safeguarding, deleting, and protecting the Private Information in  
20 its possession from being compromised, lost, stolen, accessed, and misused by  
21 unauthorized persons. MDC owed a duty to Plaintiff and Class Members to provide  
22 reasonable security, including complying with industry standards and requirements,  
23 training for its staff, and ensuring that its vendor's computer systems, networks, and  
24 protocols adequately protected the Private Information of Class Members

25        50. MDC breached its obligations to Plaintiff and Class Members and/or  
26 was otherwise negligent and reckless because it failed to properly maintain and  
27 safeguard its vendor's computer systems and data. MDC's unlawful conduct includes,  
28 but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect customers' Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to sufficiently train its employees regarding the proper handling of its customers Private Information;
- e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
- f. Failing to adhere to industry standards for cybersecurity as discussed above; and
- g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

51. MDC negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access computer network and systems which contained unsecured and unencrypted Private Information.

52. Had MDC remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

53. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with MDC.

***MDC Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft***

54. The FTC hosted a workshop to discuss “informational injuries,” which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.<sup>3</sup> Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers’ loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

55. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims’ identities in order to engage in illegal financial transactions under the victims’ names.

56. Because a person’s identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim’s identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information about a victim’s identity, such as a person’s login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to

---

<sup>3</sup> *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), available at [https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational\\_injury\\_workshop\\_staff\\_report\\_-\\_oct\\_2018\\_0.pdf](https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf) (last visited on June 17, 2024).

1 manipulate individuals into disclosing additional confidential or personal information  
2 through means such as spam phone calls and text messages or phishing emails.

3 57. In fact, as technology advances, computer programs may scan the  
4 Internet with a wider scope to create a mosaic of information that may be used to link  
5 compromised information to an individual in ways that were not previously possible.  
6 This is known as the “mosaic effect.” Names and dates of birth, combined with  
7 contact information like telephone numbers and email addresses, are very valuable to  
8 hackers and identity thieves as it allows them to access users’ other accounts.

9 58. Thus, even if certain information was not purportedly involved in the  
10 Data Breach, the unauthorized parties could use Plaintiff’s and Class Members’  
11 Private Information to access accounts, including, but not limited to, email accounts  
12 and financial accounts, to engage in a wide variety of fraudulent activity against  
13 Plaintiff and Class Members.

14 59. One such example of this is the development of “Fullz” packages.

15 60. Cybercriminals can cross-reference two sources of the Private  
16 Information compromised in the Data Breach to marry unregulated data available  
17 elsewhere to criminally stolen data with an astonishingly complete scope and degree  
18 of accuracy in order to assemble complete dossiers on individuals. These dossiers are  
19 known as “Fullz” packages.

20 61. The development of “Fullz” packages means that the stolen Private  
21 Information from the Data Breach can easily be used to link and identify it to  
22 Plaintiff’s and the proposed Class’s phone numbers, email addresses, and other  
23 sources and identifiers. In other words, even if certain information such as emails,  
24 phone numbers, or credit card or financial account numbers may not be included in  
25 the Private Information stolen in the Data Breach, criminals can easily create a Fullz  
26 package and sell it at a higher price to unscrupulous operators and criminals (such as  
27 illegal and scam telemarketers) over and over. That is exactly what is happening to  
28 Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact,



1 including this Court or a jury, to find that Plaintiff and other Class Members' stolen  
 2 Private Information are being misused, and that such misuse is fairly traceable to the  
 3 Data Breach.

4 62. For these reasons, the FTC recommends that identity theft victims take  
 5 several time-consuming steps to protect their personal and financial information after  
 6 a data breach, including contacting one of the credit bureaus to place a fraud alert on  
 7 their account (and an extended fraud alert that lasts for 7 years if someone steals the  
 8 victim's identity), reviewing their credit reports, contacting companies to remove  
 9 fraudulent charges from their accounts, placing a freeze on their credit, and correcting  
 10 their credit reports.<sup>4</sup> However, these steps do not guarantee protection from identity  
 11 theft but can only mitigate identity theft's long-lasting negative impacts.

12 63. PII is data that can be used to detect a specific individual. PII is a  
 13 valuable property right. Its value is axiomatic, considering the value of big data in  
 14 corporate America and the consequences of cyber thefts (which include heavy prison  
 15 sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII  
 16 has considerable market value.

17 64. The U.S. Attorney General stated in 2020 that consumers' sensitive  
 18 personal information commonly stolen in data breaches "has economic value."<sup>5</sup> The  
 19 increase in cyberattacks, and attendant risk of future attacks, was widely known and  
 20 completely foreseeable to the public and to anyone in Defendant's industry.

21 65. The PII of consumers remains of high value to criminals, as evidenced  
 22 by the prices they will pay through the dark web. Numerous sources cite dark web  
 23 pricing for stolen identity credentials. For example, PII can be sold at a price ranging  
 24 \_\_\_\_\_

25 <sup>4</sup> See *IdentityTheft.gov*, Federal Trade Commission, available at <https://www.identitytheft.gov/Steps>  
 26 (last visited June 17, 2024).

27 <sup>5</sup> See *Attorney General William P. Barr Announces Indictment of Four Members of China's*  
 28 *Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at <https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military> (last visited on June 17, 2024).



from \$40 to \$200, and bank details have a price range of \$50 to \$200.<sup>6</sup> Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web and that the “fullz” (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for \$30 in 2017.<sup>7</sup>

66. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that “[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails.”<sup>8</sup>

67. The Dark Web Price Index of 2022, published by PrivacyAffairs<sup>9</sup> shows how valuable just email addresses alone can be, even when not associated with a financial account:

Email Database Dumps	Avg. Price USD (2022)
10,000,000 USA email addresses	\$120
600,000 New Zealand email addresses	\$110
2,400,000 million Canada email addresses	\$100

<sup>6</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited on June 17, 2024).

<sup>7</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited on June 17, 2024).

<sup>8</sup> See <https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/> (last visited on June 17, 2024).

<sup>9</sup> See <https://www.privacyaffairs.com/dark-web-price-index-2022/> (last visited on June 17, 2024).





68. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

69. Likewise, the value of PII is increasingly evident in our digital economy. Many companies including MDC collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and shares it with third parties for similar purposes.<sup>10</sup>

70. One author has noted: “Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII.”<sup>11</sup>

71. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

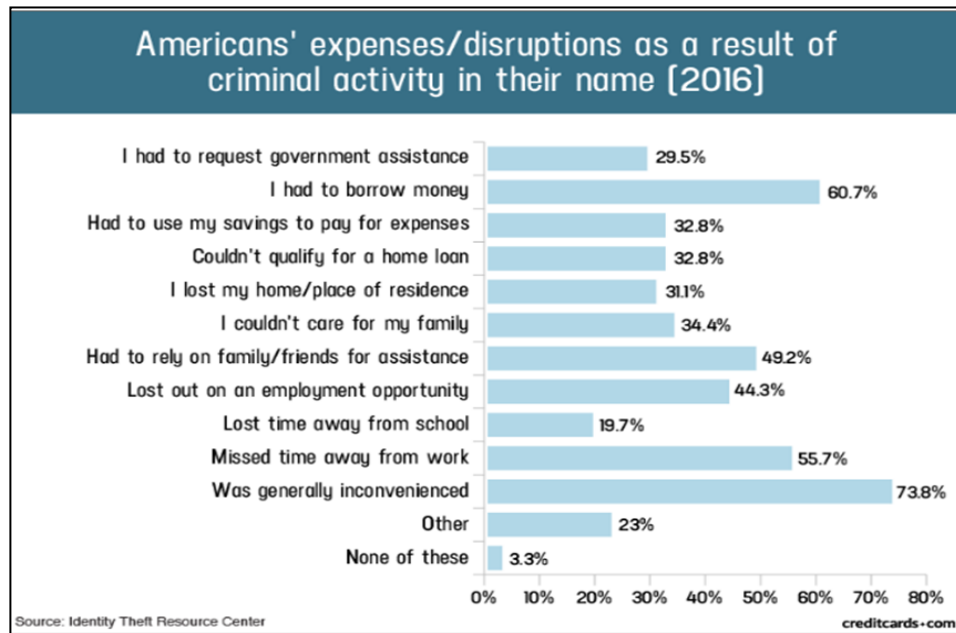
72. A consumer’s ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

73. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiff’s PII impairs her ability to participate in the economic marketplace.

<sup>10</sup> See <https://robinhood.com/us/en/support/articles/privacy-policy/> (last visited on June 17, 2024).

<sup>11</sup> See John T. Soma, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (‘PII’) Equals the “Value” of Financial Assets*, 15 Rich. J. L. & Tech. 11, 14 (2009).

74. A study by the Identity Theft Resource Center<sup>12</sup> shows the multitude of harms caused by fraudulent use of PII:



75. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:<sup>13</sup>

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

<sup>12</sup> Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), available at <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/> (last visited June 17, 2024).

<sup>13</sup> *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), available at <https://www.gao.gov/assets/270/262904.html> (last visited June 17, 2024).

1        76. PII is such a valuable commodity to identity thieves that once the  
2 information has been compromised, criminals often trade the information on the  
3 “cyber black market” for years.

4        77. As a result, Plaintiff and Class Members are at an increased risk of fraud  
5 and identity theft for many years into the future. Thus, Plaintiff and Class Members  
6 have no choice but to vigilantly monitor their accounts for many years to come.

7 ***Plaintiff's and Class Members' Damages***

8 *Plaintiff Tracy Cowherd's Experience*

9        78. Plaintiff Cowherd is unsure why MDC is in possession of her Private  
10 Information, though Defendant may have obtained her information through one of its  
11 affiliates or brand partners.

12        79. Regardless, Defendant obtained and continues to maintain Plaintiff's  
13 Private Information and has a continuing legal duty and obligation to protect that  
14 Private Information from unauthorized access and disclosure.

15        80. On or about June 5, 2024, Plaintiff Cowherd received a letter entitled  
16 “Notice of Data Breach” which told her that her Private Information had been  
17 impacted during the Data Breach. The notice letter informed her that the Private  
18 Information compromised included her “payment card information.”

19        81. The notice letter failed to offer Plaintiff Cowherd any credit monitoring  
20 or identity theft protection services. Defendant's failure to do so is insufficient given  
21 that Plaintiff Cowherd will now experience a lifetime of increased risk of identity  
22 theft and other forms of targeted fraudulent misuse of her Private Information.

23        82. Plaintiff Cowherd suffered actual injury in the form of time spent  
24 dealing with the Data Breach and the increased risk of fraud resulting from the Data  
25 Breach and/or monitoring her accounts for fraud.

26        83. Plaintiff Cowherd would not have provided her Private Information to  
27 Defendant had Defendant timely disclosed that its vendor's systems lacked adequate  
28

1 computer and data security practices to safeguard its customers' personal information  
2 from theft, and that those systems were subject to a data breach.

3 84. Plaintiff Cowherd suffered actual injury in the form of having her  
4 Private Information compromised and/or stolen as a result of the Data Breach.

5 85. Plaintiff Cowherd experienced a reduction in her credit score, and she  
6 lost considerable time at work trying to resolve her issues with her credit.

7 86. Plaintiff Cowherd suffered actual injury in the form of damages to and  
8 diminution in the value of her personal and financial information – a form of  
9 intangible property that Plaintiff Cowherd entrusted to Defendant for the purpose of  
10 receiving products and services from Defendant, which was compromised in, and as a  
11 result of, the Data Breach.

12 87. Plaintiff Cowherd suffered imminent and impending injury arising from  
13 the substantially increased risk of future fraud, identity theft, and misuse posed by her  
14 Private Information being placed in the hands of criminals.

15 88. Plaintiff Cowherd has a continuing interest in ensuring that her Private  
16 Information, which remains in the possession of Defendant, is protected and  
17 safeguarded from future breaches.

18 89. As a result of the Data Breach, Plaintiff Cowherd made reasonable  
19 efforts to mitigate the impact of the Data Breach, including but not limited to  
20 researching the Data Breach, reviewing financial accounts for any indications of  
21 actual or attempted identity theft or fraud, and researching the credit monitoring  
22 offered by Defendant, as well as long-term credit monitoring options she will now  
23 need to use. Plaintiff Cowherd has spent several hours dealing with the Data Breach,  
24 valuable time she otherwise would have spent on other activities.

25 90. As a result of the Data Breach, Plaintiff Cowherd has suffered anxiety as  
26 a result of the release of her Private Information to cybercriminals, which Private  
27 Information she believed would be protected from unauthorized access and  
28 disclosure. These feelings include anxiety about unauthorized parties viewing,

1 selling, and/or using her Private Information for purposes of committing cyber and  
2 other crimes against her. Plaintiff Cowherd is very concerned about this increased,  
3 substantial, and continuing risk, as well as the consequences that identity theft and  
4 fraud resulting from the Data Breach will have on her life.

5 91. Plaintiff Cowherd also suffered actual injury as a result of the Data  
6 Breach in the form of (a) damage to and diminution in the value of her Private  
7 Information, a form of property that Defendant obtained from Plaintiff Cowherd; (b)  
8 violation of her privacy rights; and (c) present, imminent, and impending injury  
9 arising from the increased risk of identity theft, and fraud she now faces.

10 92. As a result of the Data Breach, Plaintiff Cowherd anticipates spending  
11 considerable time and money on an ongoing basis to try to mitigate and address the  
12 many harms caused by the Data Breach.

13 93. In sum, Plaintiff and Class Members have been damaged by the  
14 compromise of their Private Information in the Data Breach.

15 94. Plaintiff and Class Members entrusted their Private Information to  
16 Defendant in order to receive Defendant's services.

17 95. Plaintiff's Private Information was subsequently compromised as a  
18 direct and proximate result of the Data Breach, which Data Breach resulted from  
19 Defendant's inadequate data security practices.

20 96. As a direct and proximate result of MDC's actions and omissions,  
21 Plaintiff and Class Members have been harmed and are at an imminent, immediate,  
22 and continuing increased risk of harm, including but not limited to, financial fraud  
23 and other forms of identity theft.

24 97. Further, as a direct and proximate result of MDC's conduct, Plaintiff and  
25 Class Members have been forced to spend time dealing with the effects of the Data  
26 Breach.

27 98. Plaintiff and Class Members also face a substantial risk of being targeted  
28 in future phishing, data intrusion, and other illegal schemes through the misuse of

1 their Private Information, since potential fraudsters will likely use such Private  
2 Information to carry out such targeted schemes against Plaintiff and Class Members.

3 99. The Private Information maintained by and stolen from Defendant's  
4 systems, combined with publicly available information, allows nefarious actors to  
5 assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to  
6 carry out targeted fraudulent schemes against Plaintiff and Class Members.

7 100. Plaintiff and Class Members also lost the benefit of the bargain they  
8 made with MDC. Plaintiff and Class Members overpaid for services that were  
9 intended to be accompanied by adequate data security but were not. Indeed, part of  
10 the price Plaintiff and Class Members paid to MDC was intended to be used by MDC  
11 to fund adequate security of MDC's system and protect Plaintiff's and Class  
12 Members' Private Information. Thus, Plaintiff and the Class did not receive what they  
13 paid for.

14 101. Additionally, as a direct and proximate result of MDC's conduct,  
15 Plaintiff and Class Members have also been forced to take the time and effort to  
16 mitigate the actual and potential impact of the data breach on their everyday lives,  
17 including placing "freezes" and "alerts" with credit reporting agencies, contacting  
18 their financial institutions, closing or modifying financial accounts, and closely  
19 reviewing and monitoring bank accounts and credit reports for unauthorized activity  
20 for years to come.

21 102. Plaintiff and Class Members may also incur out-of-pocket costs for  
22 protective measures such as credit monitoring fees, credit report fees, credit freeze  
23 fees, and similar costs directly or indirectly related to the Data Breach.

24 103. Additionally, Plaintiff and Class Members also suffered a loss of value  
25 of their PII and PHI when it was acquired by cyber thieves in the Data Breach.  
26 Numerous courts have recognized the propriety of loss of value damages in related  
27 cases. An active and robust legitimate marketplace for Private Information also  
28





exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>14</sup> In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to \$50 a year.<sup>15</sup>

104. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

105. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. The contractual bargain entered into between Plaintiff and MDC included Defendant's contractual obligation to provide adequate data security, which Defendant failed to provide. Thus, Plaintiff and Class Members did not get what they bargained for.

106. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

- a. Monitoring for and discovering fraudulent charges;

<sup>14</sup> See <https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion>. (last visited on June 17, 2024).

<sup>15</sup> *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html> (last visited June 17, 2024).



- b. Canceling and reissuing credit and debit cards;
- c. Addressing their inability to withdraw funds linked to compromised accounts;
- d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
- f. Contacting financial institutions and closing or modifying financial accounts;
- g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;
- h. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and
- i. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

107. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of MDC, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

108. As a direct and proximate result of MDC's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28

110. Specifically, Plaintiff proposes the following Nationwide Class, (referred to herein as the “Class”), subject to amendment as appropriate:

All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

112. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class, as well as add subclasses, before the Court determines whether certification is appropriate.

114. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of 89,188 customers of MDC whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through MDC's records, Class Members' records, publication notice, self-identification, and other means.

1           115. Commonality. There are questions of law and fact common to the Class  
2 which predominate over any questions affecting only individual Class Members.  
3 These common questions of law and fact include, without limitation:

- 4           a. Whether MDC engaged in the conduct alleged herein;
- 5           b. When MDC learned of the Data Breach;
- 6           c. Whether MDC's response to the Data Breach was adequate;
- 7           d. Whether MDC unlawfully lost or disclosed Plaintiff's and Class  
8           Members' Private Information;
- 9           e. Whether MDC failed to implement and maintain reasonable  
10           security procedures and practices appropriate to the nature and  
11           scope of the Private Information compromised in the Data Breach;
- 12           f. Whether MDC's data security systems prior to and during the  
13           Data Breach complied with applicable data security laws and  
14           regulations;
- 15           g. Whether MDC's data security systems prior to and during the  
16           Data Breach were consistent with industry standards;
- 17           h. Whether MDC owed a duty to Class Members to safeguard their  
18           Private Information;
- 19           i. Whether MDC breached its duty to Class Members to safeguard  
20           their Private Information;
- 21           j. Whether hackers obtained Class Members' Private Information  
22           via the Data Breach;
- 23           k. Whether MDC had a legal duty to provide timely and accurate  
24           notice of the Data Breach to Plaintiff and the Class Members;
- 25           l. Whether MDC breached its duty to provide timely and accurate  
26           notice of the Data Breach to Plaintiff and Class Members;
- 27           m. Whether MDC knew or should have known that its data security  
28           systems and monitoring processes were deficient;

- n. What damages Plaintiff and Class Members suffered as a result of MDC's misconduct;
- o. Whether MDC's conduct was negligent;
- p. Whether MDC's conduct was *per se* negligent;
- q. Whether MDC was unjustly enriched;
- r. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- s. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

116. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

117. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

118. Predominance. MDC has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from MDC's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

119. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or

1 piecemeal litigation. Absent a Class action, most Class Members would likely find  
2 that the cost of litigating their individual claims is prohibitively high and would  
3 therefore have no effective remedy. The prosecution of separate actions by individual  
4 Class Members would create a risk of inconsistent or varying adjudications with  
5 respect to individual Class Members, which would establish incompatible standards  
6 of conduct for MDC. In contrast, conducting this action as a class action presents far  
7 fewer management difficulties, conserves judicial resources and the parties'  
8 resources, and protects the rights of each Class Member.

9 120. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2).  
10 MDC has acted and/or refused to act on grounds generally applicable to the Class  
11 such that final injunctive relief and/or corresponding declaratory relief is appropriate  
12 as to the Class as a whole.

13 121. Finally, all members of the proposed Class are readily ascertainable.  
14 MDC has access to the names and addresses and/or email addresses of Class  
15 Members affected by the Data Breach. Class Members have already been  
16 preliminarily identified and sent notice of the Data Breach by MDC.

## 17 **CLAIMS FOR RELIEF**

### 18 **COUNT I**

#### 19 **NEGLIGENCE**

#### 20 **(On behalf of Plaintiff and the Nationwide Class)**

21 122. Plaintiff restates and realleges all of the allegations stated above and  
22 hereafter as if fully set forth herein.

23 123. MDC knowingly collected, came into possession of, and maintained  
24 Plaintiff's and Class Members' Private Information, and had a duty to exercise  
25 reasonable care in safeguarding, securing, and protecting such Information from  
26 being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

1 124. MDC's duty also included a responsibility to implement processes by  
2 which it could detect and analyze a breach of its vendor's security systems quickly  
3 and to give prompt notice to those affected in the case of a cyberattack.

4 125. MDC knew or should have known of the risks inherent in collecting the  
5 Private Information of Plaintiff and Class Members and the importance of adequate  
6 security. MDC was on notice because, on information and belief, it knew or should  
7 have known that it would be an attractive target for cyberattacks.

8 126. MDC owed a duty of care to Plaintiff and Class Members whose Private  
9 Information was entrusted to it. MDC's duties included, but were not limited to, the  
10 following:

- 11 a. To exercise reasonable care in obtaining, retaining, securing,  
12 safeguarding, deleting, and protecting Private Information in its  
13 possession;
- 14 b. To protect customers' Private Information using reasonable and  
15 adequate security procedures and systems compliant with industry  
16 standards;
- 17 c. To have procedures in place to prevent the loss or unauthorized  
18 dissemination of Private Information in its possession;
- 19 d. To employ reasonable security measures and otherwise protect the  
20 Private Information of Plaintiff and Class Members pursuant to the  
21 FTCA;
- 22 e. To implement processes to quickly detect a data breach and to timely  
23 act on warnings about data breaches; and
- 24 f. To promptly notify Plaintiff and Class Members of the Data Breach,  
25 and to precisely disclose the type(s) of information compromised.

26 127. MDC's duty to employ reasonable data security measures arose, in part,  
27 under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which  
28 prohibits "unfair . . . practices in or affecting commerce," including, as interpreted

1 and enforced by the FTC, the unfair practice of failing to use reasonable measures to  
2 protect confidential data.

3 128. MDC's duty also arose because Defendant was bound by industry  
4 standards to protect its customers' confidential Private Information.

5 129. Plaintiff and Class Members were foreseeable victims of any inadequate  
6 security practices on the part of Defendant, and MDC owed them a duty of care to not  
7 subject them to an unreasonable risk of harm.

8 130. MDC, through its actions and/or omissions, unlawfully breached its duty  
9 to Plaintiff and Class Members by failing to exercise reasonable care in protecting  
10 and safeguarding Plaintiff's and Class Members' Private Information within MDC's  
11 possession.

12 131. MDC, by its actions and/or omissions, breached its duty of care by  
13 failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate  
14 computer systems and data security practices to safeguard the Private Information of  
15 Plaintiff and Class Members.

16 132. MDC, by its actions and/or omissions, breached its duty of care by  
17 failing to promptly identify the Data Breach and then failing to provide prompt notice  
18 of the Data Breach to the persons whose Private Information was compromised.

19 133. MDC breached its duties, and thus was negligent, by failing to use  
20 reasonable measures to protect Class Members' Private Information. The specific  
21 negligent acts and omissions committed by Defendant include, but are not limited to,  
22 the following:

- 23 a. Failing to adopt, implement, and maintain adequate security measures to
- 24 safeguard Class Members' Private Information;
- 25 b. Failing to adequately monitor the security of its vendor's networks and
- 26 systems;
- 27 c. Failing to periodically ensure that its email system maintained
- 28 reasonable data security safeguards;



- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to comply with the FTCA;
- f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

134. MDC acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiff and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

135. MDC had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust MDC with their Private Information was predicated on the understanding that MDC would take adequate security precautions. Moreover, only MDC had the ability to protect its customers' Private Information from a cyberattack.

136. MDC's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

137. MDC's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

138. As a result of MDC's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

1 139. MDC also had independent duties under state laws that required it to  
2 reasonably safeguard Plaintiff's and Class Members' Private Information and  
3 promptly notify them about the Data Breach.

4 140. As a direct and proximate result of MDC's negligent conduct, Plaintiff  
5 and Class Members have suffered damages as alleged herein and are at imminent risk  
6 of further harm.

7 141. The injury and harm that Plaintiff and Class Members suffered was  
8 reasonably foreseeable.

9 142. Plaintiff and Class Members have suffered injury and are entitled to  
10 damages in an amount to be proven at trial.

11 143. In addition to monetary relief, Plaintiff and Class Members are also  
12 entitled to injunctive relief requiring MDC to, *inter alia*, strengthen its data security  
13 systems and monitoring procedures, conduct periodic audits of those systems, and  
14 provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class  
15 Members.

## 16 COUNT II

### 17 NEGLIGENCE *PER SE*

#### 18 (On behalf of Plaintiff and the Nationwide Class)

19 144. Plaintiff restates and realleges the allegations in the preceding  
20 paragraphs as if fully set forth herein.

21 145. Pursuant to Section 5 of the FTCA, MDC had a duty to provide fair and  
22 adequate computer systems and data security to safeguard the Private Information of  
23 Plaintiff and Class Members.

24 146. MDC breached its duties by failing to employ industry-standard  
25 cybersecurity measures in order to comply with the FTCA, including but not limited  
26 to proper segregation, access controls, password protection, encryption, intrusion  
27 detection, secure destruction of unnecessary data, and penetration testing.

1 147. Plaintiff and Class Members are within the class of persons that the  
2 FTCA is intended to protect.

3 148. The FTCA prohibits “unfair . . . practices in or affecting commerce,”  
4 including, as interpreted and enforced by the FTC, the unfair act or practice of failing  
5 to use reasonable measures to protect PII (such as the Private Information  
6 compromised in the Data Breach). The FTC rulings and publications described  
7 above, together with the industry-standard cybersecurity measures set forth herein,  
8 form part of the basis of MDC’s duty in this regard.

9 149. MDC violated the FTCA by failing to use reasonable measures to protect  
10 the Private Information of Plaintiff and the Class and by not complying with  
11 applicable industry standards, as described herein.

12 150. It was reasonably foreseeable, particularly given the growing number of  
13 data breaches of Private Information, that the failure to reasonably protect and secure  
14 Plaintiff’s and Class Members’ Private Information in compliance with applicable  
15 laws would result in an unauthorized third-party gaining access to MDC’s networks,  
16 databases, and computers that stored Plaintiff’s and Class Members’ unencrypted  
17 Private Information.

18 151. MDC’s violations of the FTCA constitute negligence *per se*.

19 152. Plaintiff’s and Class Members’ Private Information constitutes personal  
20 property that was stolen due to MDC’s negligence, resulting in harm, injury, and  
21 damages to Plaintiff and Class Members.

22 153. As a direct and proximate result of MDC’s negligence *per se*, Plaintiff  
23 and the Class have suffered, and continue to suffer, injuries and damages arising from  
24 the unauthorized access of their Private Information, including but not limited to  
25 damages from the lost time and effort to mitigate the actual and potential impact of  
26 the Data Breach on their lives.

27 154. MDC breached its duties to Plaintiff and the Class under the FTCA by  
28 failing to provide fair, reasonable, or adequate computer systems and data security

practices to safeguard Plaintiff's and Class Members' Private Information.

155. As a direct and proximate result of MDC's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

156. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring MDC to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

### **COUNT III**

#### **BREACH OF CONTRACT**

##### **(On behalf of Plaintiff and the Nationwide Class)**

157. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

158. Plaintiff and Class Members entered into a valid and enforceable contract through which they paid money to MDC in exchange for services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiff's and Class Members' Private Information.

159. MDC's Privacy Policy memorialized the rights and obligations of MDC and its customers. This document was provided to Plaintiff and Class Members in a manner in which it became part of the agreement for services.

160. In the Privacy Policy, MDC commits to protecting the privacy and security of private information and promises to never share Plaintiff's and Class Members' Private Information except under certain limited circumstances.

161. Plaintiff and Class Members fully performed their obligations under their contracts with MDC.

162. However, MDC did not secure, safeguard, and/or keep private Plaintiff's and Class Members' Private Information, and therefore MDC breached its contracts

1 with Plaintiff and Class Members.

2 163. MDC allowed third parties to access, copy, and/or exfiltrate Plaintiff's  
3 and Class Members' Private Information without permission. Therefore, MDC  
4 breached the Privacy Policy with Plaintiff and Class Members.

5 164. MDC's failure to satisfy its confidentiality and privacy obligations  
6 resulted in MDC providing services to Plaintiff and Class Members that were of a  
7 diminished value.

8 165. As a result, Plaintiff and Class Members have been harmed, damaged,  
9 and/or injured as described herein, including in Defendant's failure to fully perform  
10 its part of the bargain with Plaintiff and Class Members.

11 166. As a direct and proximate result of MDC's conduct, Plaintiff and Class  
12 Members suffered and will continue to suffer damages in an amount to be proven at  
13 trial.

14 167. In addition to monetary relief, Plaintiff and Class Members are also  
15 entitled to injunctive relief requiring MDC to, *inter alia*, strengthen its data security  
16 systems and monitoring procedures, conduct periodic audits of those systems, and  
17 provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class  
18 Members.

19 **COUNT IV**

20 **BREACH OF IMPLIED CONTRACT**

21 **(On behalf of Plaintiff and the Nationwide Class)**

22 168. Plaintiff restates and realleges the allegations in the preceding  
23 paragraphs as if fully set forth herein.

24 169. This Count is pleaded in the alternative to Count III above.

25 170. MDC provides online consumer goods and services to Plaintiff and  
26 Class Members. Plaintiff and Class Members formed an implied contract with  
27 Defendant regarding the provision of those services through their collective conduct,  
28

1 including by Plaintiff and Class Members paying for goods and services from  
2 Defendant.

3 171. Through Defendant's sale of goods and services, it knew or should have  
4 known that it must protect Plaintiff's and Class Members' confidential Private  
5 Information in accordance with MDC's policies, practices, and applicable law.

6 172. As consideration, Plaintiff and Class Members paid money to MDC and  
7 turned over valuable Private Information to MDC. Accordingly, Plaintiff and Class  
8 Members bargained with MDC to securely maintain and store their Private  
9 Information.

10 173. MDC accepted possession of Plaintiff's and Class Members' Private  
11 Information for the purpose of providing goods and services to Plaintiff and Class  
12 Members.

13 174. In delivering their Private Information to MDC and paying for goods and  
14 services, Plaintiff and Class Members intended and understood that MDC would  
15 adequately safeguard the Private Information as part of that service.

16 175. Defendant's implied promises to Plaintiff and Class Members include,  
17 but are not limited to, (1) taking steps to ensure that anyone who is granted access to  
18 Private Information also protect the confidentiality of that data; (2) taking steps to  
19 ensure that the Private Information that is placed in the control of its employees is  
20 restricted and limited to achieve an authorized business purpose; (3) restricting access  
21 to qualified and trained employees and/or agents; (4) designing and implementing  
22 appropriate retention policies to protect the Private Information against criminal data  
23 breaches; (5) applying or requiring proper encryption; (6) implementing multifactor  
24 authentication for access; and (7) taking other steps to protect against foreseeable data  
25 breaches.

26 176. Plaintiff and Class Members would not have entrusted their Private  
27 Information to MDC in the absence of such an implied contract.  
28

1 177. Had MDC disclosed to Plaintiff and the Class that they did not have  
2 adequate computer systems and security practices to secure sensitive data, Plaintiff  
3 and Class Members would not have provided their Private Information to MDC.

4 178. MDC recognized that Plaintiff's and Class Member's Private  
5 Information is highly sensitive and must be protected, and that this protection was of  
6 material importance as part of the bargain to Plaintiff and the other Class Members.

7 179. MDC violated these implied contracts by failing to employ reasonable  
8 and adequate security measures to secure Plaintiff's and Class Members' Private  
9 Information.

10 180. Plaintiff and Class Members have been damaged by MDC's conduct,  
11 including the harms and injuries arising from the Data Breach now and in the future,  
12 as alleged herein.

13 **COUNT V**

14 **INTRUSION UPON SECLUSION / INVASION OF PRIVACY**

15 **(On behalf of Plaintiff and the Nationwide Class)**

16 181. Plaintiff restates and realleges the allegations in the preceding  
17 paragraphs as if fully set forth herein.

18 182. Plaintiff and Class Members maintain a privacy interest in their Private  
19 Information, which is private, confidential information that is also protected from  
20 disclosure by applicable laws set forth above.

21 183. Plaintiff and Class Members' Private Information was contained, stored,  
22 and managed electronically in MDC's records, computers, and databases that was  
23 intended to be secured from unauthorized access to third-parties because highly  
24 sensitive, confidential matters regarding Plaintiff's and Class Members' identities  
25 were only shared with MDC for the limited purpose of obtaining and paying for  
26 Defendant's services.



1 184. Additionally, Plaintiff's and Class Members' Private Information is  
2 highly attractive to criminals who can nefariously use such Private Information for  
3 fraud, identity theft, and other crimes without the victims' knowledge and consent.

4 185. MDC's disclosure of Plaintiff's and Class Members' Private Information  
5 to unauthorized third parties as a result of its failure to adequately secure and  
6 safeguard their Private Information is offensive. MDC's disclosure of Plaintiff's and  
7 Class Members' Private Information to unauthorized third parties permitted the  
8 physical and electronic intrusion into private quarters where Plaintiff's and Class  
9 Members' Private Information was stored.

10 186. Plaintiff and Class Members have been damaged by MDC's conduct,  
11 including by incurring the harms and injuries arising from the Data Breach now and  
12 in the future.

### 13 **COUNT VI**

#### 14 **UNJUST ENRICHMENT**

#### 15 **(On behalf of Plaintiff and the Nationwide Class)**

16 187. Plaintiff restates and realleges the allegations in the preceding  
17 paragraphs as if fully set forth herein.

18 188. This Count is pleaded in the alternative to Counts III and IV above.

19 189. Plaintiff and Class Members conferred a benefit on MDC by turning  
20 over their Private Information to Defendant and by paying for products and services  
21 that should have included cybersecurity protection to protect their Private  
22 Information. Plaintiff and Class Members did not receive such protection.

23 190. Upon information and belief, MDC funds its data security measures  
24 entirely from its general revenue, including from payments made to it by Plaintiff and  
25 Class Members.

26 191. As such, a portion of the payments made by Plaintiff and Class Members  
27 is to be used to provide a reasonable and adequate level of data security that is in  
28 compliance with applicable state and federal regulations and industry standards, and

1 the amount of the portion of each payment made that is allocated to data security is  
2 known to MDC.

3 192. MDC has retained the benefits of its unlawful conduct, including the  
4 amounts of payment received from Plaintiff and Class Members that should have  
5 been used for adequate cybersecurity practices that it failed to provide.

6 193. MDC knew that Plaintiff and Class Members conferred a benefit upon it,  
7 which MDC accepted. MDC profited from these transactions and used the Private  
8 Information of Plaintiff and Class Members for business purposes, while failing to  
9 use the payments it received for adequate data security measures that would have  
10 secured Plaintiff's and Class Members' Private Information and prevented the Data  
11 Breach.

12 194. If Plaintiff and Class Members had known that MDC had not adequately  
13 secured their Private Information, they would not have agreed to provide such Private  
14 Information to Defendant.

15 195. Due to MDC's conduct alleged herein, it would be unjust and  
16 inequitable under the circumstances for MDC to be permitted to retain the benefit of  
17 its wrongful conduct.

18 196. As a direct and proximate result of MDC's conduct, Plaintiff and Class  
19 Members have suffered and will suffer injury, including but not limited to: (i) the loss  
20 of the opportunity to control how their Private Information is used; (ii) the  
21 compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket  
22 expenses associated with the prevention, detection, and recovery from identity theft,  
23 and/or unauthorized use of their Private Information; (iv) lost opportunity costs  
24 associated with effort expended and the loss of productivity addressing and  
25 attempting to mitigate the actual and future consequences of the Data Breach,  
26 including but not limited to efforts spent researching how to prevent, detect, contest,  
27 and recover from identity theft; (v) the continued risk to their Private Information,  
28 which remains in MDC's possession and is subject to further unauthorized

disclosures so long as MDC fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

197. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from MDC and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by MDC from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

198. Plaintiff and Class Members may not have an adequate remedy at law against MDC, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

## **COUNT VII**

### **DECLARATORY JUDGMENT**

#### **(On behalf of Plaintiff and the Nationwide Class)**

199. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

200. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal statutes described in this Complaint.

201. MDC owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

202. MDC still possesses Private Information regarding Plaintiff and Class Members.

203. Plaintiff alleges that MDC's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her Private Information and the risk remains that further compromises of her Private Information will occur in the future.

204. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. MDC owes a legal duty to secure its customers' Private Information and to timely notify customers of a data breach under the common law and Section 5 of the FTCA;
- b. MDC's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect customers' Private Information; and
- c. MDC continues to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

205. This Court should also issue corresponding prospective injunctive relief requiring MDC to employ adequate security protocols consistent with legal and industry standards to protect customers' Private Information, including the following:

- a. Order MDC to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.
- b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, MDC must implement and maintain reasonable security measures, including, but not limited to:
  - i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on MDC's systems on a periodic basis, and ordering MDC to promptly correct any problems or issues detected by such third-party security auditors;

- ii. engaging third-party security auditors and internal personnel to run automated security monitoring;
- iii. auditing, testing, and training its security personnel regarding any new or modified procedures;
- iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of MDC's systems;
- v. conducting regular database scanning and security checks;
- vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- vii. meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps MDC's customers should take to protect themselves.

206. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at MDC. The risk of another such breach is real, immediate, and substantial. If another breach at MDC occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

207. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to MDC if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of MDC's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and MDC has a pre-existing legal obligation to employ such measures.

208. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a

subsequent data breach at MDC, thus preventing future injury to Plaintiff and other customers whose Private Information would be further compromised.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of herself and the Class described above, seeks the following relief:

- a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;
- b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
- d. An order instructing MDC to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;
- e. An order requiring MDC to pay the costs involved in notifying Class Members about the judgment and administering the claims process;
- f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and
- g. An award of such other and further relief as this Court may deem just and proper.

//

//

//

//

**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury on all triable issues.

DATED this 18th day of June 2024.

Respectfully submitted,

**KAZEROUNI LAW GROUP, APC**

By: /s/ Mona Amini

Mona Amini, Esq.  
Gustavo Ponce, Esq.  
6940 S. Cimarron Road, Suite 210  
Las Vegas, Nevada 89113  
Telephone: (800) 400-6808  
Facsimile: (800) 520-5523  
Email: mona@kazlg.com  
Email: gustavo@kazlg.com

Mason A. Barney  
Tyler J. Bean  
**SIRI & GLIMSTAD LLP**  
745 Fifth Avenue, Suite 500  
New York, New York 10151  
Telephone: (212) 532-1091  
Email: mbarney@sirillp.com  
Email: tbean@sirillp.com

*Attorneys for Plaintiff*

